BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646)-837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: sbogdanovich@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA—WESTERN DIVISION

REBEKKA LIEN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

OYO HOTELS INC.,

Defendant.

Case No. 2:25-cv-1785

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Rebekka Lien files this class action complaint on behalf of herself and all others similarly situated (the "Class Members") against Oyo Hotels Inc. ("Defendant" or "Oyo"). Plaintiff brings this action based on personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all California residents who have accessed and used oyorooms.com (the "Website"), a website that Defendant owns and operates.

2. Defendant aids, employs, agrees with, or otherwise enables a third party – Google LLC ("Google") – to eavesdrop on communications sent and received by Plaintiff and Class Members, including communications that contain sensitive and confidential information (i.e., "guest records," as defined by Cal. Civil Code § 53.5). By failing to procure consent before enabling Google's interception of these communications, Defendant violated the California Invasion of Privacy Act ("CIPA") §§ 631-632.

PARTIES

3. Plaintiff Rebekka Lien is a resident and citizen of Alhambra, California. Several times, including on or around April 3, 2024, Plaintiff Lien visited Defendant's Website, oyorooms.com, on the same browser that she used to access Google's products and services[1] (including Gmail). Plaintiff Lien was in California when she visited the Website. Upon accessing the Website, as alleged in greater detail below, Plaintiff Lien browsed and booked an Oyo hotel. Each of these communications was intercepted in transit by Google – as enabled by Defendant – including communications that contained Plaintiff Lien's confidential "guest records," as defined by Cal. Civil Code § 53.5. Neither Defendant nor Google procured Plaintiff

[1] *See* GOOGLE, PRODUCTS, https://about.google/intl/ALL_us/products/.

Lien's prior consent to this interception.

4. Defendant Oyo Hotels Inc. is a Delaware corporation with its principal place of business at 1920 McKinney Avenue, 7th Floor, Dallas, Texas 75201. Defendant does business across the nation and operates numerous hotels throughout California.[2]

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action where there are more than 100 members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one member of the putative Class is a citizen of a state different from Defendant.

6. The Court has personal jurisdiction over Defendant because Defendant has purposefully availed itself of the laws and benefits of doing business in California, and Plaintiff's claims arise out of Defendant's forum-related activities. Plaintiff accessed and navigated the Website while in California, and Defendant assisted Google with intercepting Plaintiff's communications in this District.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial portion of the events giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

I. The California Invasion of Privacy Act

8. The California Legislature enacted the Invasion of Privacy Act to protect certain privacy rights of California citizens. The legislature expressly recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications … has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

[2] https://www.oyorooms.com/us/allcities/.

9. The California Supreme Court has repeatedly stated an "express objective" of CIPA is to "protect a person placing or receiving a call from a situation where the person on the other end of the line *permits an outsider to tap his telephone or listen in on the call*." *Ribas v. Clark*, 38 Cal. 3d 355, 364 (1985) (emphasis added).

10. Further, as the California Supreme Court has held in explaining the legislative purpose behind CIPA:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.*
>
> As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribas v. Clark, 38 Cal. 3d 355, 360-61 (1985) (emphasis added; internal citations omitted).

11. As part of CIPA, the California Legislature enacted § 631(a), which prohibits any person or entity from [i] "intentionally tap[ping], or mak[ing] any unauthorized connection … with any telegraph or telephone wire," [ii] "willfully and without the consent of all parties to the communication … read[ing], or attempt[ing] to read, or to learn the contents or meaning of any … communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within [California]," or [iii] "us[ing], or attempt[ing] to use … any information so obtained."

12. CIPA § 631(a) also penalizes [iv] those who "aid[], agree[] with, employ[], or conspire[] with any person" who conducts the aforementioned wiretapping, or those who "permit" the wiretapping.

13. As part of the Invasion of Privacy Act, the California Legislature additionally introduced Penal Code § 632(a), which prohibits any person or entity from "intentionally and without the consent of all parties to a confidential communication, us[ing] an electronic amplifying or recording device to eavesdrop upon or record [a] confidential communication."

14. A "confidential communication" for the purposes of CIPA § 632 is "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." Cal. Penal Code § 632(c).

15. Individuals may bring an action against the violator of CIPA §§ 631 and 632 for $5,000 per violation. Cal. Penal Code § 637.2(a)(1). Plaintiff does so, here, against Defendant.

II. California Civil Code § 53.5

16. As the California Legislature recognized, a "guest record" maintained by an owner or operator of an inn, hotel, motel, lodginghouse, or other similar accommodations is confidential. Such an owner or operator "shall not disclose, produce, provide, release, transfer, disseminate, or otherwise communicate, except to a California peace officer, all or any part of a guest record orally, in writing, or by electronic or any other means to a third party without a court-issued subpoena, warrant, or order." Cal. Civil Code § 53.5(a).

17. Per Cal. Civil Code § 53.5(c):

> "Guest record" for purposes of this section includes any record that identifies an individual guest, boarder, occupant, lodger, customer, or invitee, including, but not limited to, their name, social security number or other unique identifying number, date of birth, location of birth, address, telephone number, driver's license number, other official form of identification, credit card number, or automobile license plate number.

18. Further, the legislative history of § 53.5 indicates:

(a) In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use of their personal information.

(b) Since California voters approved the right of privacy, the California Legislature has adopted specific mechanisms to safeguard consumer privacy, including the California Consumer Privacy Act of 2018, the Online Privacy Protection Act, the Reader Privacy Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California law intended to give Californians the 'who, what, where, and when' of how businesses handle consumers' personal information.

(c) Californians frequently have to disclose their sensitive personal information to third parties in order to accomplish routine activities: apply for a job; apply for housing; raise a child; drive a car or take transportation; or stay at a hotel or motel.

(d) California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information by third parties.

(e) Many businesses collect personal information from California consumers. They may know where a consumer lives, how many children a consumer has, where a consumer lives and works, where a consumer travels and where they stay on their trip, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories.

(f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, including financial fraud, identity theft, unnecessary costs to

> personal time and finances, destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.
>
> (g) When Californians leave their homes to travel via bus or stay at lodging establishments throughout their state, they desire assurances that these businesses will respect their privacy and safeguard their personal information from improper disclosure.
>
> (h) Protecting the privacy of personal information promotes consumer confidence and encourages both residents and visitors to travel to and within California and to patronize California businesses.
>
> (i) Therefore, it is the intent of the Legislature to further Californians' right to privacy by ensuring that the personal information disclosed by patrons of lodging establishments and bus companies is used for the intended business purposes and not improperly disclosed.

California S.B. 1194 (September 27, 2018).[3]

19. Here, Website users' communications with Oyo – made while browsing and booking Oyo hotels via the Website – contain sensitive and confidential "guest records," as defined by Cal. Civil Code § 53.5.

20. First, the communications include "record[s] that identif[y] an individual[.]" Cal. Civil Code § 53.5(c). As described *infra*, §§ IV, VI, Defendant enables Google to identify individual Website users with Google Analytics identity spaces – a combination of user IDs, user-provided data (i.e., contact details like email address, phone number, name, and/or address, etc.), device IDs, and/or machine learning-based behavioral modeling – and Google signals (which associates web browsing activity with users' Google accounts). These pieces of data collected by Google constitute "record[s] that identif[y] an individual" (Cal. Civil Code § 53.5(c)), as they contain "unique identifying number[s]" assigned to Website users

[3] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id= 201720180SB1194.

(*id.*) and other personal information associated with Website users. *Id.*

21. Website users' communications with Oyo also "identif[y] an individual [as an Oyo] guest, boarder, occupant, lodger, customer, or invitee[.]" *Id.* Google intercepts Website users' button clicks selecting the destination to which they wish to travel, the desired dates for their trip, the number of rooms they require, the numbers of adults and children who will be traveling, and the particular hotel and room type in which they wish to stay. Google also intercepts the URL of webpages visited by Website users – containing the foregoing communications. These communications "identif[y] an individual [as an Oyo] guest, boarder, occupant, lodger, customer, or invitee" (Cal. Civil Code § 53.5(c)) because they show that all Website users are "invitees" of Oyo – individuals with "express or implied invitation to enter or use [Oyo's] premises."[4] These communications also identify certain Website users (those who complete the booking process) as Oyo hotel "guests" and "customers."

22. Thus, Google – as aided by Defendant – intercepted "guest records," which are confidential, under Cal. Civil Code § 53.5. Moreover, Google is not a legitimate "third-party service provider," as defined by Cal. Civil Code § 53.5(f), because Google is not "an entity contracted to provide services outlined in [a] contract [with Oyo] that has no independent right to use or share the data beyond the terms of the contract." Rather, Google has the capability to use the information it wiretaps for purposes other than simply providing a recording to Defendant. *See infra*, § VII. Therefore, Defendant's conduct here at issue was not permitted by, *inter alia*, Cal. Civil Code § 53.5(i).

III. Overview of Defendant's Website

23. Defendant owns and operates the Website. Defendant has integrated Google's wiretaps into the Website.

24. On the Website, Website users can, *inter alia*, browse and book Oyo

[4] INVITEE, Black's Law Dictionary (11th ed. 2019).

hotels. When doing so, Website users provide Defendant with confidential information, including "guest records" under Cal. Civil Code § 53.5. *See supra* § II.

25. Unbeknownst to Plaintiff and Class Members, however, Defendant aids, agrees with, employs, or otherwise enables Google to eavesdrop on those confidential communications using Google's wiretaps, as set out *infra*.

26. Website users' confidential communications are the product of Website users affirmatively entering, and interacting with, information on the Website (*i.e.*, the confidential communications are not procedurally or automatically generated). Instead, as set out below, the confidential communications stem from Website users typing into data fields, conveying responses to questions and prompts, and actively making other selections. All of the foregoing is information created through the intent of Website users: information created by and in response to Website users' communicative inputs; information created by and in response to Website users' intended messages to the Website and Defendant; and information created by and in response to Website users' having conveyed and expressed their respective desires that the Website would supply them with certain, highly personalized, types of information and/or responses.

27. Website users may browse and book Oyo hotel rooms. To do so, users type and/or select from a list the destination to which they wish to travel. Next, users click the dates for their trip, the number of rooms required, the number of adults and children who will be traveling, and/or special rates for which they are eligible. Google, as enabled by Defendant, contemporaneously intercepts Website users' button clicks selecting such items:

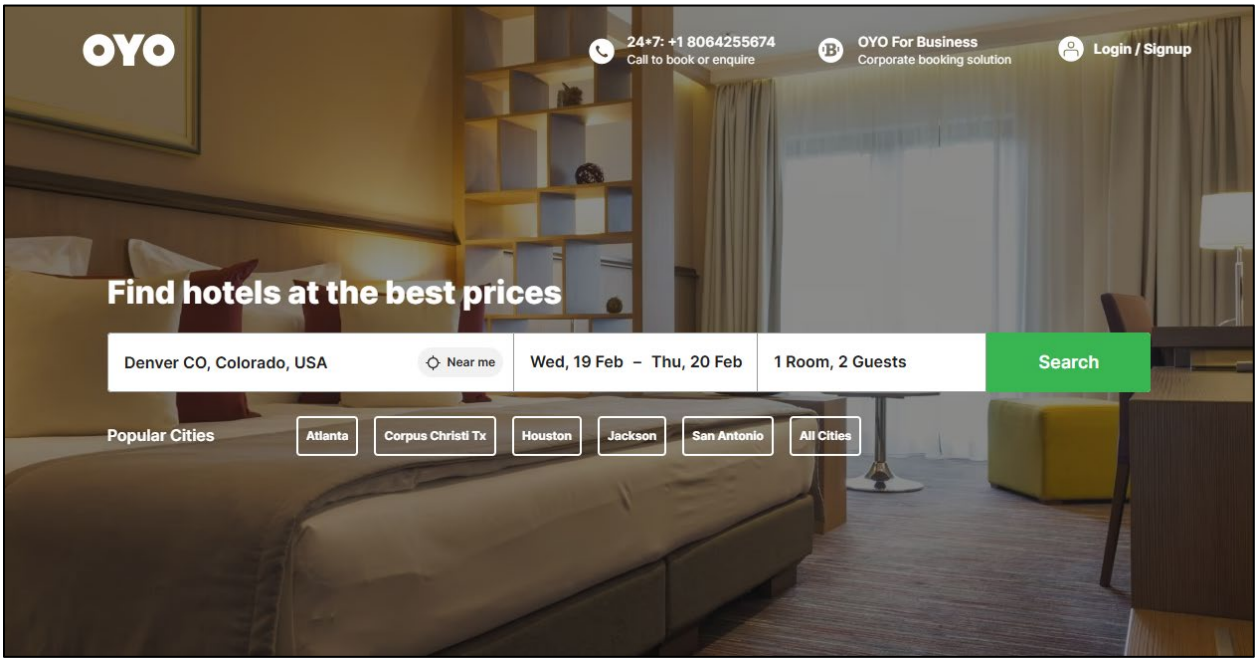
//

//

//

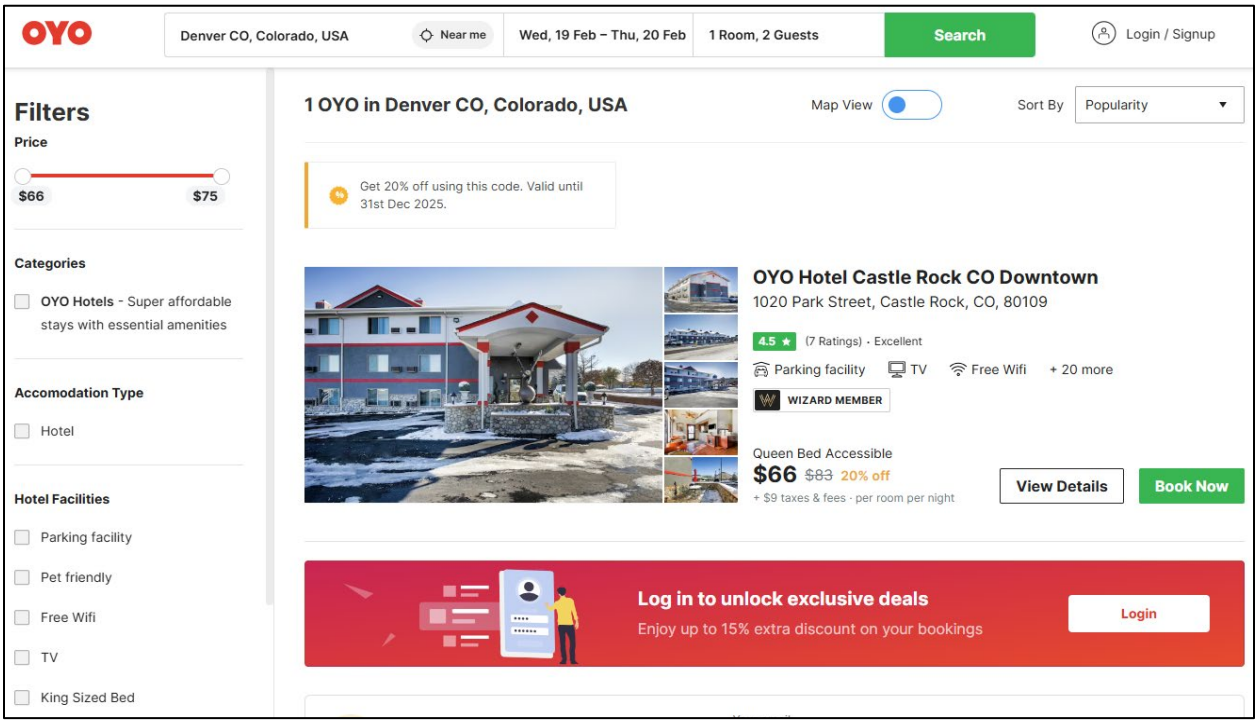
//

//



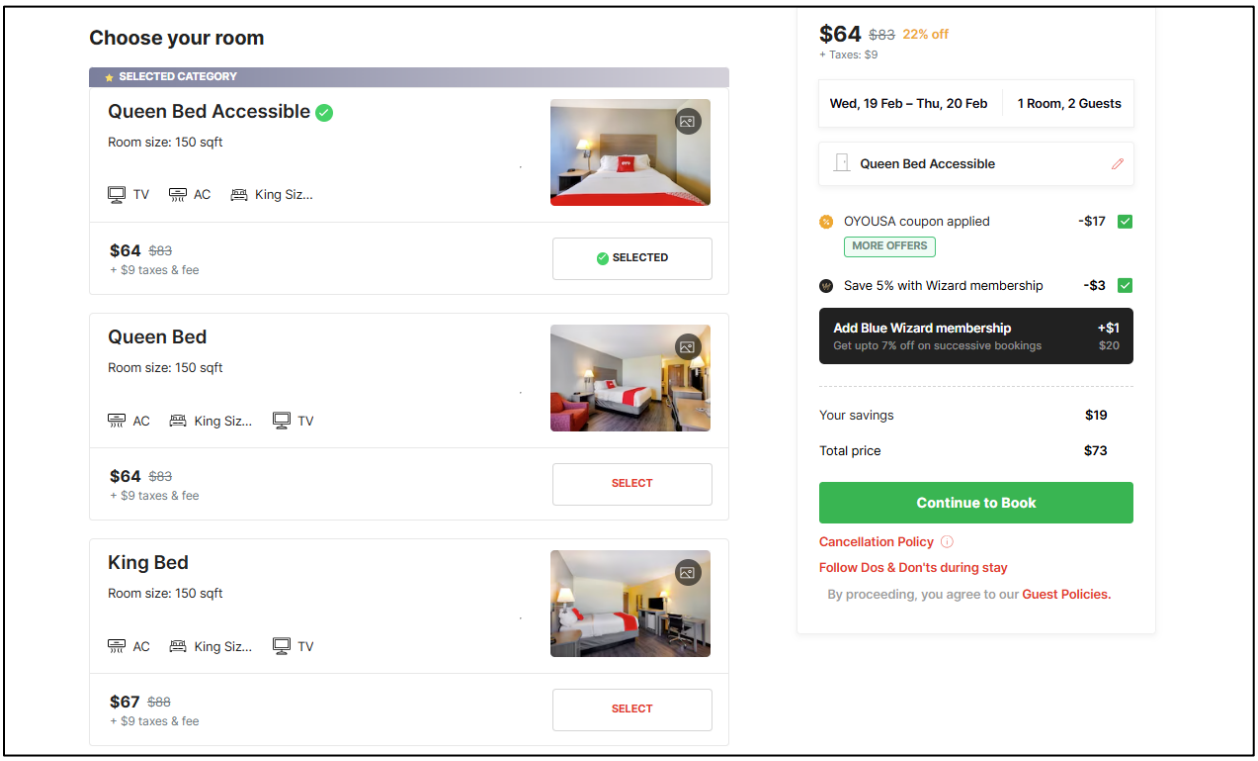
Website "Screen 1"

28. Then, Website users review the Oyo hotels located in or near their destination and click on a particular hotel to book.



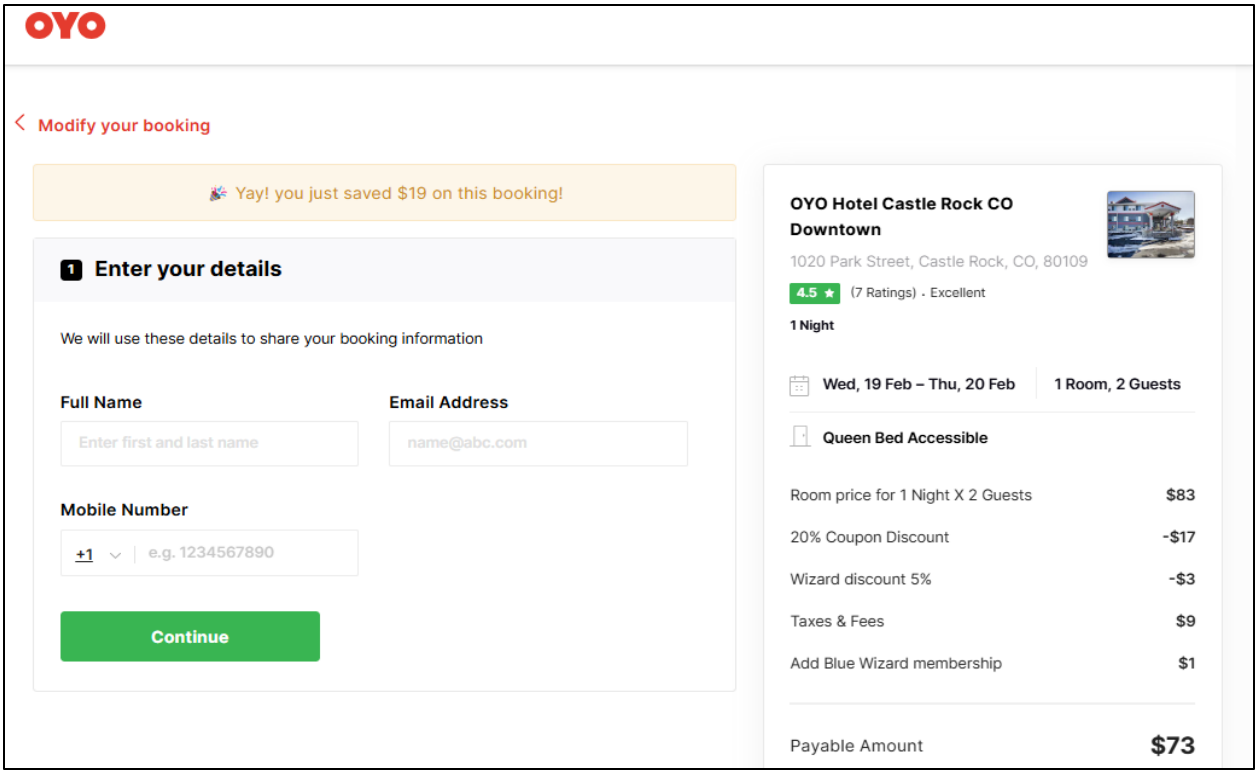
Website "Screen 2"

29. Website users subsequently pick the type of room (i.e., double, queen, king bed, etc.) in which they wish to stay.



Website "Screen 3"

30. Finally, Website users check out by typing their personal information (first and last name, email, phone number) and entering their payment information.



Website "Screen 4"

IV. Overview of Google's Tracking Technologies

A. Background

31. Google wiretaps the Website with its tracking technologies, which Defendant purposefully installed on the Website.

32. Google's tracking technologies send secret instructions to a Website user's browser, without alerting the individual that this is happening. The trackers then cause the browser to secretly and simultaneously duplicate the user's Website communications, transmitting these communications to Google's servers alongside additional information about the Website user's identity. This entire process occurs within milliseconds. In other words, when a user communicates with Defendant's Website, those communications are simultaneously and contemporaneously duplicated and sent to Google at the same time as they are being sent to Defendant. Thus, Google's interception of these communications occurs "in transit." *See, e.g.*, *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) ("Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion…"); *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019) ("Even if the browser caused a parallel signal to be sent to NaviStone, that intervention happened while the signal was already in transit from Revitch's device. Section 631's protections extend explicitly to the beginnings and ends of communications…"); *James v. Walt Disney Co.*, 710 F. Supp. 3d 942, 961-62 (N.D. Cal. 2023) (finding in-transit interception was alleged based on similar process to the one alleged herein).

B. Google Analytics

33. Google wiretaps the Website with trackers associated with "Google Analytics."[5] According to Google, "Google Analytics is a platform that collects data

[5] GOOGLE, START LEARNING ABOUT GOOGLE ANALYTICS, https://developers.google.com/analytics.

from [] websites and apps to create reports that provide insights into [] business[es].”[6] “To measure a website … [one] add[s] a small piece of JavaScript measurement code to each page on [a] site.”[7] Then, “[e]very time a user visits a webpage, the tracking code will collect … information about how that user interacted with the page.”[8] Specifically, Google Analytics tracks “events”; “sessions”; and “users[.]”[9]

34. “Events let [clients] measure … when someone loads a page, clicks a link, [] makes a purchase[]” and more.[10] Google provides a menu of “recommended events” (i.e., “completes a purchase”; “searches [] website or app”; “select content on [] website or app”; “views an item”; “views their shopping cart”)[11] and also allows for “collect[ing] additional information that Google Analytics does not collect automatically[,]” through “custom events.”[12]

35. A “session” is “the period from when a user visits [a] website or app to when they leave [said] website or app[.][13] “When a session starts, Google automatically collects a session_start event and generates a session ID (ga_session_id) and session number (ga_session_number)[.]”[14]

---

[6] GOOGLE, HOW GOOGLE ANALYTICS WORKS, https://support.google.com/analytics/answer/12159447.

[7] *Id.*

[8] *Id.*

[9] GOOGLE, TRAFFIC-SOURCE DIMENSIONS, https://support.google.com/analytics/answer/11080067.

[10] GOOGLE, SET UP EVENTS, https://developers.google.com/analytics/devguides/collection/ga4/events.

[11] GOOGLE, [GA4] RECOMMENDED EVENTS, https://support.google.com/analytics/answer/9267735.

[12] GOOGLE, [GA4] CUSTOM EVENTS, https://support.google.com/analytics/answer/12229021.

[13] GOOGLE, TRAFFIC-SOURCE DIMENSIONS, https://support.google.com/analytics/answer/11080067.

[14] GOOGLE, [GA4] ABOUT ANALYTICS SESSIONS, https://support.google.com/analytics/answer/9191807.

36. Finally, to discern when "two different [users] interact with [a] website[,] … Google Analytics identifies an individual user based on [Google Analytics] reporting identit[ies.]"[15] Reporting identities are combinations of "identifiers … called *identity spaces*" – namely, "User-ID"; "user-provided data"; "device ID"; and "modeling[.]"[16]

- A "User-ID" is a "persistent ID[,]"[17] consisting of a unique combination of up to "256 characters[,]"that is created by website operators and "assign[ed] and consistently reassign[ed] … to [] users[,] … typically [] during login."[18]
- "User-provided data" consists of contact details such as "email, phone, name and address[,]" provided by website users, that "is [] matched with other Google data … to improve the accuracy of [] measurement data and power enhanced Analytics capabilities."[19] Although these personal details are "hashed,"[20] the reality is that, even in hashed form, they are traceable to individuals.[21]

---

[15] GOOGLE, TRAFFIC-SOURCE DIMENSIONS, https://support.google.com/analytics/answer/11080067.

[16] GOOGLE, [GA4] REPORTING IDENTITIES, https://support.google.com/analytics/answer/10976610.

[17] *Id.*

[18] GOOGLE, [GA4] MEASURE ACTIVITY ACROSS PLATFORMS WITH USER-ID, https://support.google.com/analytics/answer/9213390.

[19] GOOGLE, [GA4] USER-PROVIDED DATA COLLECTION, https://support.google.com/analytics/answer/14077171.

[20] *Id.*

[21] *See, e.g.*, FEDERAL TRADE COMMISSION, DOES HASHING MAKE DATA "ANONYMOUS"?, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2012/04/does-hashing-make-data-anonymous ("[H]ashing is vastly overrated as an 'anonymization' technique … the casual assumption that hashing is sufficient to anonymize data is risky at best, and usually wrong."); FEDERAL TRADE COMMISSION, NO, HASHING STILL DOESN'T MAKE YOUR DATA ANONYMOUS, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/07/no-hashing-still-doesnt-make-your-data-anonymous ("[H]ashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymized."); STEVEN ENGLEHARDT ET AL., I NEVER SIGNED UP FOR THIS! PRIVACY IMPLICATIONS OF EMAIL TRACKING, https://petsymposium.org/2018/files/papers/issue1/paper42-2018-1-

- A "device ID" is a "browser-based or mobile-app-based identifier[.]"[22] "On a website, device ID gets its value from the client ID property of the _ga cookie. In an iOS or Firebase app, device ID gets its value from the app-instance ID, which identifies a unique installation of the app."[23]

- "Modeling" uses "machine learning to model the behavior of users who decline analytics cookies based on the behavior of similar users who accept analytics cookies."[24]

37. Google Analytics can also leverage "Google signals," which "associates [data] with user[s'] … Google accounts," for "users who have signed in … and who have turned on Ads Personalization."[25] "This association of data with these signed-in users is used to enable cross-device remarketing, and cross-device key events export to Google Ads."[26]

V. Defendant Aids, Agrees with, Employs, or Otherwise Enables Google to Wiretap Californians' Communications

38. Google, as enabled by Defendant, contemporaneously intercepts the following Website communications.

//

//

---

source.pdf ("[H]ashing of PII, including emails, is not a meaningful privacy protection. This is folk knowledge in the security community, but bears repeating."); MARTECH, FTC PRIVACYCON: YOUR EMAIL ADDRESS IS LEAKING AND VULNERABLE, https://martech.org/ftc-privacycon-email-address-leaking-vulnerable ("Hashing is an algorithmic process that turns [information] into a gibberish label[.] … Although gibberish, it's unique, so it can be employed as an anonymized identifier. It's supposed to be one-way, meaning that you can't turn the gibberish back into the [original form]. Wrong, says Englehardt and his colleagues.").

[22] GOOGLE, [GA4] DEVICE ID, https://support.google.com/analytics/answer/9356035.

[23] *Id.*

[24] GOOGLE, [GA4] BEHAVIORAL MODELING FOR CONSENT MODE, https://support.google.com/analytics/answer/11161109.

[25] GOOGLE, [GA4] ACTIVATE GOOGLE SIGNALS FOR GOOGLE ANALYTICS PROPERTIES, https://support.google.com/analytics/answer/9445345.

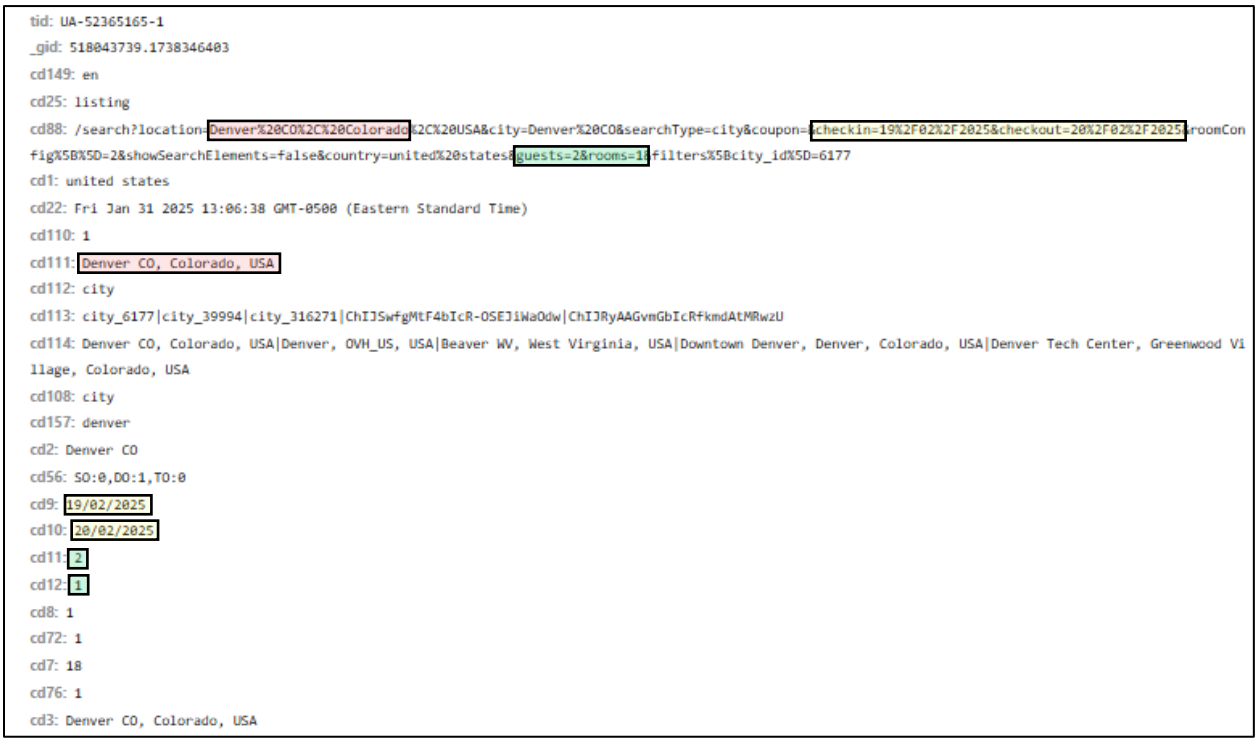
[26] *Id.*

dl: https://www.oyorooms.com/us/
dt: OYO Hotels USA, Starting at $30 - Book Direct for Guaranteed Best Rate
en: Home_Page
_ee: 1
ep.event_label: Search Widget
ep.event_action: Clicked
epn.event_value: 0
ep.custom_label: Suggestion city Selected | Denver CO, Colorado, USA
ep.dimension22: Fri Jan 31 2025 13:00:55 GMT-0500 (Eastern Standard Time)
ep.nonInteraction: true
_et: 38
tfd: 54736

dl: https://www.oyorooms.com/us/
dt: OYO Hotels USA, Starting at $30 - Book Direct for Guaranteed Best Rate
en: Home_Page
_ee: 1
ep.event_label: Calendar
ep.event_action: Clicked
epn.event_value: 0
ep.custom_label: Check-in Selected
ep.dimension2: Denver CO
ep.dimension56: 1
ep.dimension112: city
ep.dimension9: 19/02/2025
ep.dimension10: 01/02/2025

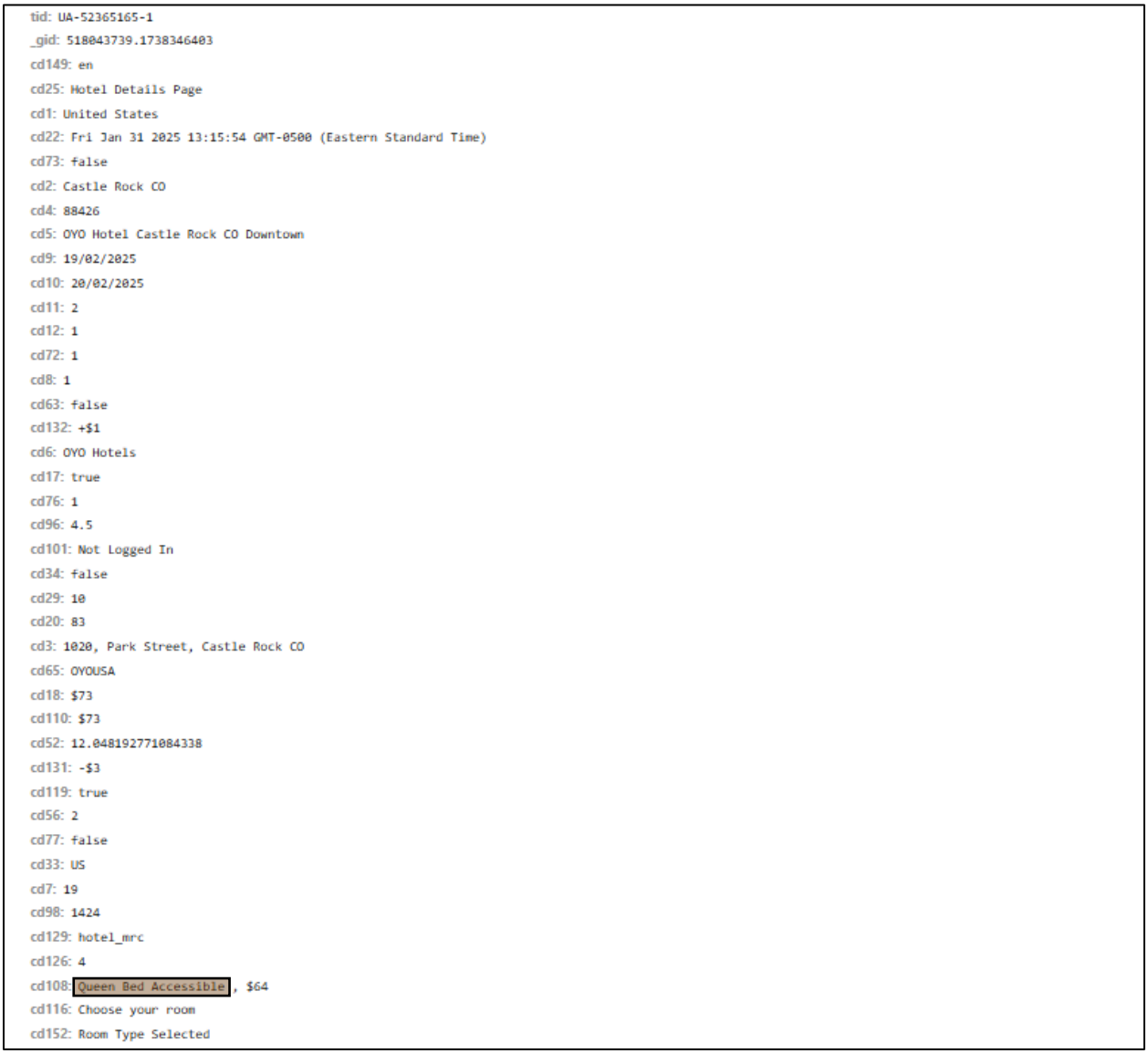
dl: https://www.oyorooms.com/us/
dt: OYO Hotels USA, Starting at $30 - Book Direct for Guaranteed Best Rate
en: Home_Page
_ee: 1
ep.event_label: Calendar
ep.event_action: Clicked
epn.event_value: 0
ep.custom_label: Check-out selected
ep.dimension2: Denver CO
ep.dimension56: 1
ep.dimension112: city
ep.dimension9: 19/02/2025
ep.dimension10: 20/02/2025

dl: https://www.oyorooms.com/us/
dt: OYO Hotels USA, Starting at $30 - Book Direct for Guaranteed Best Rate
en: Home_Page
_ee: 1
ep.event_label: Room And Guests
ep.event_action: Clicked
epn.event_value: 0
ep.custom_label: Add Guests Clicked | 1 to 2



39. As shown by the red highlights in the above excerpt of the Website's transmissions, Google intercepts the destination selected by users (here, "Denver CO"). As shown by the yellow highlights, Google intercepts the desired trip dates selected by users (here, "Check-in" of "19/02/2025" and "Check-out" of "20/02/2025"). As shown by the green highlight, Google intercepts the numbers of rooms and guests selected by users (here, "guests=2" and "rooms=1").

40. As shown by the purple highlight in the above excerpt of the Website's transmissions, Google intercepts the particular Oyo hotel selected by users (here, "Oto Hotel Castle Rock CO Downtown"). This communications is the product of a button click on Website Screen 2.



41. As shown by the brown highlight in the above excerpt of the Website's transmissions, Google intercepts the room type selected by users (here, "Queen Bed Accessible"). This communication is the product of a button click on Website Screen 3.

//

```
dl: https://www.oyorooms.com/search?location=Denver%20CO%2C%20Colorado%2C%20USA&city=Denver%20CO&searchType=city&checkin=19%2F02%2F2025&checkout=20%2F02%2
F2025&roomConfig%5B%5D=2&guests=2&rooms=1&filters%5Bcity_id%5D=6177
dr: https://www.oyorooms.com/us/
dt: Hotels in Denver CO Starting @ $66 - Upto 20% OFF on 1 Denver CO Hotels
en: Listing_Page
_ee: 1
ep.event_label: [Free Wifi]
ep.event_action: Clicked
epn.event_value: 0
ep.custom_label: Hotel Facilities Filter Applied
```

```
dl: https://www.oyorooms.com/us/88426/?checkin=19%2F02%2F2025&checkout=20%2F02%2F2025&rooms=1&guests=2&rooms_config=1-2_0&selected_rcid=272884
ul: en-us
de: UTF-8
dt: OYO Hotel Castle Rock CO Downtown in Castle Rock CO| Book @ $63 and Get 33% Off
sd: 24-bit
sr: 1920x1080
vp: 1384x1037
je: 0
ec: Hotel Gallery Page
ea: Horizontal Gallery Open
el: View All Images
```

```
dl: https://www.oyorooms.com/us/88426/?checkin=19%2F02%2F2025&checkout=20%2F02%2F2025&rooms=1&guests=2&rooms_config=1-2_0&selected_rcid=272884
ul: en-us
de: UTF-8
dt: OYO Hotel Castle Rock CO Downtown in Castle Rock CO| Book @ $63 and Get 33% Off
sd: 24-bit
sr: 1920x1080
vp: 1384x1037
je: 0
ec: Hotel Gallery Page
ea: Horizontal Gallery Tab Clicked
el: Reception
```

42. As shown by the orange highlights in the above excerpts of the Website's transmissions, Google intercepts miscellaneous other selections by users (here, "Free Wi-fi" as in filtering for a hotel with free Wi-Fi; "View All Images" as in opening a gallery of hotel photos; and "Reception" as in looking at photos of a hotel's reception area). These communications are the products of button clicks on Website Screens 2 and 3.

VI. Defendant Enables Google to Pair the Above Data with Users' Identities

43. As discussed *supra*, § IV, the Google tracking technologies at issue can pair wiretapped data with website users' identities.

44. To do so, the Google Analytics identity spaces and Google signals rely, at least in part, on Google cookies.[27] A cookie is a "small text file (up to 4KB) created

[27] *See, e.g.*, GOOGLE, OUR ADVERTISING AND MEASUREMENT COOKIES, https://business.safety.google/adscookies/; GOOGLE, GOOGLE ANALYTICS COOKIE USAGE ON WEBSITES, https://web.archive.org/web/20240303080533/https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage; OPEN COOKIE DATABASE, https://jkwakman.github.io/Open-Cookie-Database/open-cookie-database.html.

by a website that is stored in the user's computer either temporarily for that session only or permanently in storage (persistent cookie)."[28] Persistent cookies can be used to "track user behavior across different sites. They store information such as geographic location, device specifications, and specific actions taken on the website."[29] Thus, together, the Google cookies allow Google Analytics to "'remember' what a user has done on previous pages [and their] interactions with the [W]ebsite."[30]

45. The following image confirms that, when a user accesses the Website while logged in to a Google account, the Google tracking technologies on the Website compel that user's browser to transmit several Google cookies, including the AMP_TOKEN; ar_debug; DSID; _ga; _ga_<wpid>; _gid; IDE; NID; _Secure-1PAPISID; _Secure-1PSID; _Secure-1PSIDCC; _Secure-1PSIDTS; _Secure-3PAPISID; _Secure3PSID; _Secure-3PSIDCC; and _Secure-3PSIDTS cookies:

//

//

//

//

//

//

//

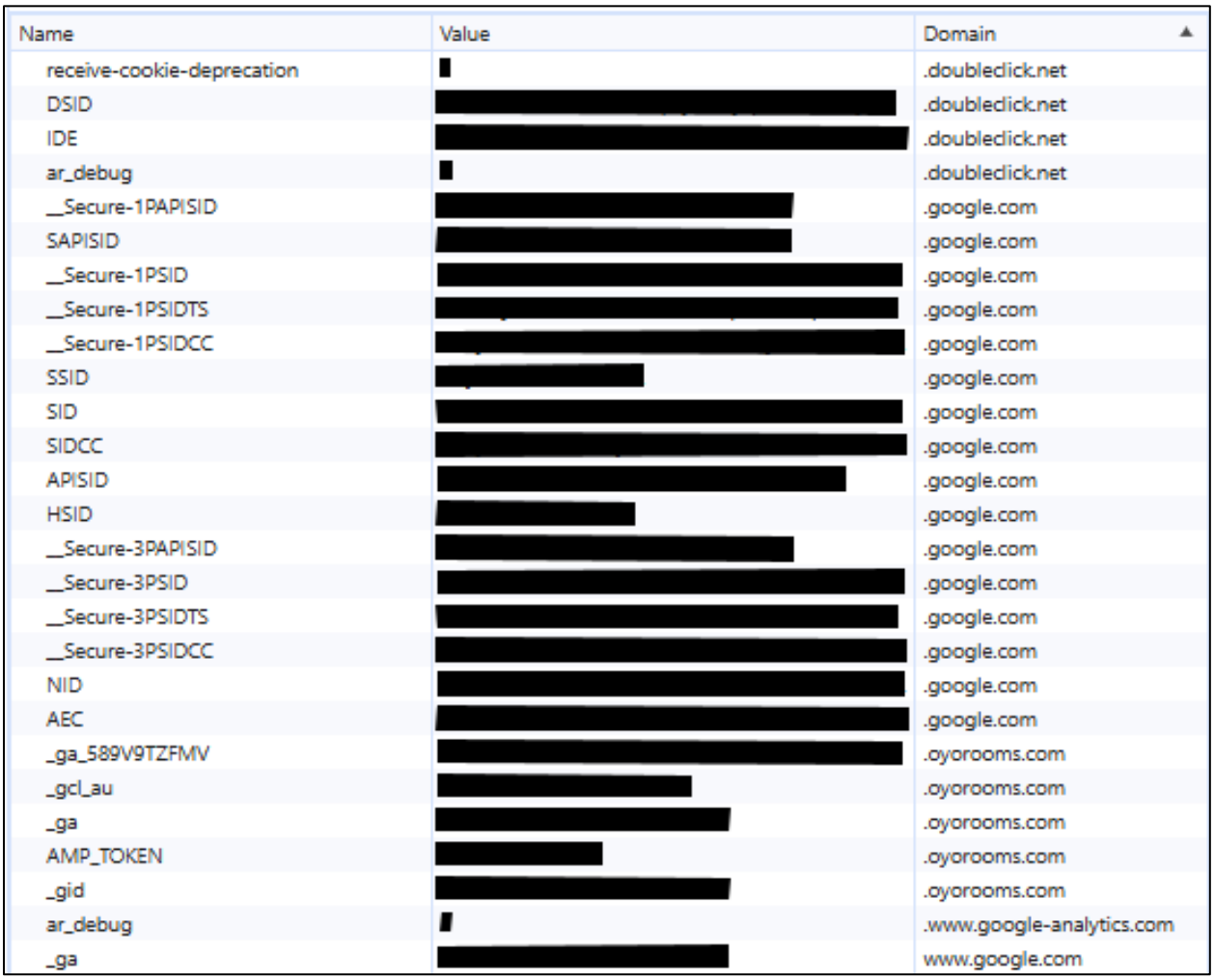
//

//

[28] PC MAGAZINE, COOKIE TABLE, https://www.pcmag.com/encyclopedia/term/cookie.

[29] COOKIEBOT, WHAT ARE TRACKING COOKIES AND HOW DO THEY WORK?, https://www.cookiebot.com/en/tracking-cookies/.

[30] GOOGLE, GOOGLE ANALYTICS COOKIE USAGE ON WEBSITES, https://web.archive.org/web/20240303080533/https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage.



Name	Value	Domain
receive-cookie-deprecation	[redacted]	.doubleclick.net
DSID	[redacted]	.doubleclick.net
IDE	[redacted]	.doubleclick.net
ar_debug	[redacted]	.doubleclick.net
__Secure-1PAPISID	[redacted]	.google.com
SAPISID	[redacted]	.google.com
__Secure-1PSID	[redacted]	.google.com
__Secure-1PSIDTS	[redacted]	.google.com
__Secure-1PSIDCC	[redacted]	.google.com
SSID	[redacted]	.google.com
SID	[redacted]	.google.com
SIDCC	[redacted]	.google.com
APISID	[redacted]	.google.com
HSID	[redacted]	.google.com
__Secure-3PAPISID	[redacted]	.google.com
__Secure-3PSID	[redacted]	.google.com
__Secure-3PSIDTS	[redacted]	.google.com
__Secure-3PSIDCC	[redacted]	.google.com
NID	[redacted]	.google.com
AEC	[redacted]	.google.com
_ga_589V9TZFMV	[redacted]	.oyorooms.com
_gcl_au	[redacted]	.oyorooms.com
_ga	[redacted]	.oyorooms.com
AMP_TOKEN	[redacted]	.oyorooms.com
_gid	[redacted]	.oyorooms.com
ar_debug	[redacted]	.www.google-analytics.com
_ga	[redacted]	www.google.com

46. The AMP_TOKEN cookie "[c]ontains a code that is used to read out a Client ID from the AMP Client ID Service. By matching this ID with that of Google Analytics, users can be matched when switching between AMP content and non-AMP content."[31] The AMP_TOKEN cookie has a lifespan of between 30 seconds and 1 year.[32]

47. The ar_debug cookie is used to "[s]tore and track conversions[.]"[33] The ar_debug cookie has a lifespan of 90 days.[34]

---

[31] OPEN COOKIE DATABASE, https://jkwakman.github.io/Open-Cookie-Database/open-cookie-database.html.

[32] *Id.*

[33] *Id.*

[34] GOOGLE, OUR ADVERTISING AND MEASUREMENT COOKIES, https://business.safety.google/adscookies.

48. The DSID cookie "[i]dentifies signed-in users on non-Google sites[.]"[35] The DSID cookie has a lifespan of 2 weeks.

49. The _ga and ga_<wpid> cookies are "used to identifier users[.]"[36] The _ga and ga_<wpid> cookies have a lifespan of 2 years.[37]

50. The _gid cookie is "used to identify users for 24 hours after last activity[.]"[38] The _gid cookie has a lifespan of 24 hours.[39]

51. The IDE cookie "is used for targeting, analyzing, and optimization of ad campaigns in DoubleClick/Google Marketing Suite."[40] The IDE cookie has a lifespan of 2 years.[41]

52. The NID cookie "is used to collect website statistics and track conversion rates and Google ad personalization[.]"[42] The NID cookie has a lifespan of 1 year.[43]

53. The _Secure-1PAPISID; _Secure-1PSID; _Secure-1PSIDC; and _Secure-1PSIDTS cookies are "[t]argeting cookie[s u]sed to create a user profile and display relevant and personalised Google Ads to the user."[44] The _Secure-1PAPISID; _Secure-1PSID; _Secure-1PSIDC; and _Secure-1PSIDTS cookies have a lifespan of 2 years.[45]

54. The _Secure-3PAPISID cookie "[p]rofiles the interests of website

---

[35] OPEN COOKIE DATABASE, https://jkwakman.github.io/Open-Cookie-Database/open-cookie-database.html.

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

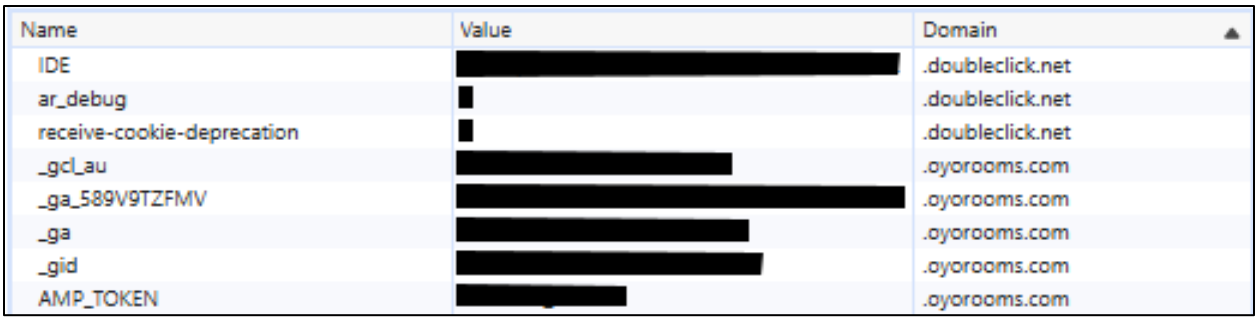
[45] *Id.*

visitors to serve relevant and personalised ads through retargeting."[46] The _Secure-3PAPISID cookie has a lifespan of 2 years.[47]

55. The _Secure3PSID cookie is a "[t]argeting cookie[u]sed to profile the interests of website visitors and display relevant and personalised Google ads."[48] The _Secure3PSID cookie has a lifespan of 2 years.[49]

56. The _Secure-3PSIDCC and _Secure-3PSIDTS cookies are "[t]argeting cookie[s u]sed to create a user profile and display relevant and personalised Google Ads to the user."[50] The _Secure-3PSIDCC and _Secure-3PSIDTS cookies have a lifespan of 2 years.[51]

57. Even when a when a user accesses the Website while not logged in to a Google account, the Google tracking technologies on the Website compel that user's browser to transmit several Google cookies, including the AMP_TOKEN; _ga; _ga_<wpid>; _gid; and IDE cookies:



58. Defendant also uses Google signals, which "associates [data] with user[s'] … Google accounts," for "users who have signed in … [and] turned on Ads Personalization."[52] The blue line below shows that Defendant enabled Google signals.

---

[46] *Id.*

[47] *Id.*

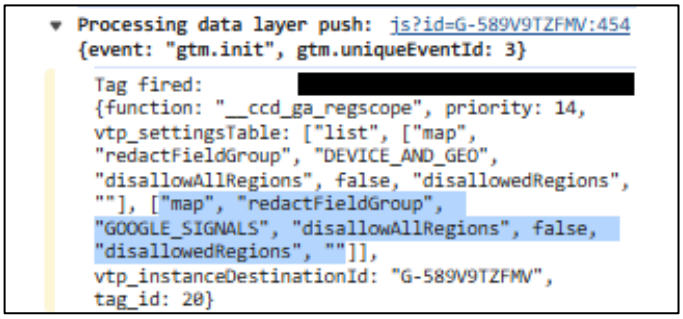
[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] GOOGLE, [GA4] ACTIVATE GOOGLE SIGNALS FOR GOOGLE ANALYTICS PROPERTIES, https://support.google.com/analytics/answer/9445345.



VII. Google Uses Californians' Data for its Own Purposes

59. When Google uses its wiretaps on Website users' communications, the wiretaps are not like tape recorders or "tools" used by one party to record the other. Instead, Google – a separate and distinct entity from the parties to the conversations – uses the wiretaps to eavesdrop upon, record, extract data from, and analyze conversations to which it is not a party. Google itself, collects the contents of said conversations. That data is then analyzed by Google before being provided to any entity that was a party to the conversations (like Defendant).

60. Google has the capability to use the contents of conversations it collect through its wiretaps for its own purposes.

61. In its "Shared Data Under Measurement Controller-Controller Data Protection Terms," Google states: "When Google Analytics customers enable the data sharing setting for … Google Analytics[] and accept the 'Measurement Controller-Controller Data Protection Terms' … Google can access and analyze the Analytics data customers share with us to better understand online behavior and trends, and improve our products and services—for example, to improve Google search results, detect and remove invalid advertising traffic in Google Ads, and test algorithms and build models that power services like Google Analytics Intelligence that apply machine-learning to surface suggestions and insights for customers based on their analytics data and like Google Ads that applies broad models to improve ads personalization and relevance."[53] Thus, Google has the capability to use the

[53] GOOGLE, SHARED DATA UNDER MEASUREMENT CONTROLLER-CONTROLLER DATA PROTECTION TERMS, https://support.google.com/analytics/answer/9024351.

wiretapped data for understanding online behavior and trends, machine learning, and improving its products and services.

VIII. Defendant Never Received Users' Consent to Disclose their Confidential Communications to Google

62. Crucially, neither Defendant nor Google procures prior consent from Californians for Google to engage in this wiretapping.

63. Nowhere on the Website does Defendant provide notice of its privacy-related practices that is prominently displayed, designed to attract Website users' attention, and distinctive in appearance.

64. Nowhere on the Website does Defendant adequately disclose the tracking here at issue, including that:

- Google, as enabled by Defendant, intercepts the contents of Californians' communications on the Website, in real time.
- These communications include, but are not limited to, "guest records," which are affirmatively entered by users on the Website and confidential under Cal. Civil Code § 53.5(c). Namely, Google intercepts Website users' button clicks selecting the destination to which they wish to travel, the desired dates for their trip, the number of rooms they require, the numbers of adults and children who will be traveling, and the particular hotel and room type in which they wish to stay. Google also intercepts the URLs of webpages visited by Website users – containing the foregoing communications.
- This information is not anonymized because Defendant enables Google to link users' communications with personal information that reveals their identities. Such personal information includes Google Analytics identity spaces – a combination of user IDs, user-provided data (i.e., contact details like email address, phone number, name, and/or address, etc.), device IDs, and/or machine learning-based behavioral modeling – and Google signals (which associates web browsing activity with users' Google accounts). These are "record[s] that identif[y] an individual[.]" Cal. Civil Code § 53.5(c).

65. Nowhere on the Website does Defendant request or receive Website users' affirmative consent *prior to* enabling Google's tracking technologies. Analysis

of the Website reveals that Google's tracking technologies are active as soon as the Website loads, before Website users could even conceivably be put on notice or provide affirmative consent.

CLASS ALLEGATIONS

66. Plaintiff seeks certification of the following class: all California residents who have accessed and navigated the Website while in California (the "Class").

67. Plaintiff reserves the right to modify the Class definition, including by using subclasses, as appropriate based on further investigation and discovery obtained in the case.

68. The following people are excluded from the Class: (1) any Judge presiding over this action and members of her or her family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest (including current and former employees, officers, or directors); (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

69. **Numerosity:** The number of persons within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class render joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

70. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that

predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary between members of the Class, and which may be determined without reference to the individual circumstances of any Class member, include, but are not limited to, the following: whether Defendant violated CIPA §§ 631 and 632 and whether Plaintiff and the proposed Class members are entitled to damages, reasonable attorneys' fees, pre-judgment interest and costs of this suit.

71. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other class members, visited the Website and had her confidential electronic communications intercepted and disclosed to Google.

72. **Adequate Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained competent counsel experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and her counsel.

73. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Classes. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will

ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSES OF ACTION

COUNT I
Violation of the California Invasion of Privacy Act, Cal. Penal Code § 631(a)

74. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

75. Plaintiff brings this Count individually and on behalf of the members of the Class.

76. CIPA § 631(a) imposes liability for "distinct and mutually independent patterns of conduct." *Tavernetti v. Superior Ct.*, 22 Cal. 3d 187, 192-93 (1978). Thus, to establish liability under CIPA § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> *Or*
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> *Or*
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> *Or*

> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

77. CIPA § 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *see also Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications.").

78. Google's tracking technologies associated with Google Analytics are a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

79. Google is a "separate legal entity that offers [a] 'software-as-a-service' and not merely a passive device." *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 520 (C.D. Cal. 2021). Further, Google has the capability to use the wiretapped information for its own purposes. Accordingly, Google was a third party to any communication between Plaintiff and Class Members, on the one hand, and Defendant, on the other. *Id*. at 521; *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023).

80. At all relevant times, by its tracking technologies, Google willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, attempted to read, and/or learned the contents or meaning of electronic communications of Plaintiff and Class Members, on the one hand, and Defendant, on the other, while the electronic communications were in transit or were being sent from or received at any place within California.

81. At all relevant times, Google used or attempted to use the

communications intercepted by their tracking technologies for its own purposes.

82. At all relevant times, Defendant aided, agreed with, employed, permitted, or otherwise enabled Google to wiretap Plaintiff and Class Members using Google's tracking technologies and to accomplish the wrongful conduct at issue here.

83. Plaintiff and Class Members did not provide their prior consent to Google's intentional access, interception, reading, learning, recording, collection, and usage of Plaintiff's and Class Members' electronic communications. Nor did Plaintiff and Class Members provide their prior consent to Defendant aiding, agreeing with, employing, permitting, or otherwise enabling Google's conduct.

84. The wiretapping of Plaintiff and Class Members occurred in California, where Plaintiff and Class Members accessed the Website and where Google – as enabled by Defendant – routed Plaintiff's and Class Members' electronic communications to Google's servers.

85. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 631(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 631(a).

COUNT II
Violation of the California Invasion of Privacy Act, Cal. Penal Code § 632

86. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

87. Plaintiff brings this Count individually and on behalf of the members of the Class.

88. CIPA § 632(a) prohibits an entity from:

> intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

89. Google's tracking technologies are "electronic amplifying or recording device[s]." *Id.*

90. Cal. Civ. Code § 53.5(a) states:

> [A]n innkeeper, hotelkeeper, motelkeeper, lodginghouse keeper, or owner or operator of an inn, hotel, motel, lodginghouse, or other similar accommodations, or any employee or agent thereof, who offers or accepts payment for rooms, sleeping accommodations, or board and lodging, or other similar accommodation, shall not disclose, produce, provide, release, transfer, disseminate, or otherwise communicate, except to a California peace officer, all or any part of a guest record orally, in writing, or by electronic or any other means to a third party without a court-issued subpoena, warrant, or order.

91. Per Cal. Civil Code § 53.5(c):

> "Guest record" for purposes of this section includes any record that identifies an individual guest, boarder, occupant, lodger, customer, or invitee, including, but not limited to, their name, social security number or other unique identifying number, date of birth, location of birth, address, telephone number, driver's license number, other official form of identification, credit card number, or automobile license plate number.

92. Here, Website users' communications with Defendant – made while browsing and booking Oyo hotels via the Website – contain sensitive and confidential "guest records," as defined by Cal. Civil Code § 53.5.

93. First, the communications include "record[s] that identif[y] an individual[.]" Cal. Civil Code § 53.5(c). Defendant enables Google to identify individual Website users with Google Analytics identity spaces – a combination of user IDs, user-provided data (i.e., contact details like email address, phone number, name, and/or address, etc.), device IDs, and/or machine learning-based behavioral modeling – and Google signals (which associates web browsing activity with users' Google accounts). These pieces of data collected by Google constitute "record[s] that identif[y] an individual" (Cal. Civil Code § 53.5(c)), as they contain "unique

identifying number[s]" assigned to Website users (*id.*) and other personal information associated with Website users. *Id.*

94. Second, Website users' communications with Oyo "identif[y] an individual [as an Oyo] guest, boarder, occupant, lodger, customer, or invitee[.]" *Id.* Google intercepts Website users' button clicks selecting the destination to which they wish to travel, the desired dates for their trip, the number of rooms they require, the numbers of adults and children who will be traveling, and the particular hotel and room type in which they wish to stay. Google also intercepts the URL of webpages visited by Website users – containing the foregoing communications. These communications "identif[y] an individual [as an Oyo] guest, boarder, occupant, lodger, customer, or invitee" (Cal. Civil Code § 53.5(c)) because they show that all Website users are "invitees" of Oyo – individuals with "express or implied invitation to enter or use [Oyo's] premises."[54] These communications also identify certain Website users (those who complete the booking process) as Oyo hotel "guests" and "customers."

95. Thus, Google – as aided by Defendant – intercepted "guest records," which are confidential, under Cal. Civil Code § 53.5. Moreover, Google is not a legitimate "third-party service provider," as defined by Cal. Civil Code § 53.5(f), because Google is not "an entity contracted to provide services outlined in [a] contract [with Oyo] that has no independent right to use or share the data beyond the terms of the contract." Rather, Google has the capability to use the information it wiretaps for purposes other than simply providing a recording to Defendant. Therefore, Defendant's conduct here at issue was not permitted by, *inter alia*, Cal. Civil Code § 53.5(i).

96. When communicating with Defendant, Plaintiff and Class Members had an objectively reasonable expectation of privacy, based on Cal. Civil Code § 53.5. Thus, Plaintiff and Class Members did not reasonably expect that anyone other than Defendant would be on the other end of the communication, and that other, third-party

[54] INVITEE, Black's Law Dictionary (11th ed. 2019).

entities like Google would intentionally use an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

97. Plaintiff and Class Members did not consent to any of Google's actions. Nor have Plaintiff or Class Members consented to Google's intentional use of an electronic amplifying or recording device to eavesdrop upon and record the confidential communications of Plaintiff and Class Members.

98. Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 632(a), and each seeks statutory damages of $5,000 for each of Defendant's violations of CIPA § 632(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order certifying the Class, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order declaring that Defendant's conduct violates the statute referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For actual, compensatory, statutory, and/or punitive in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper; and

(h) For an order awarding Plaintiff and the Class their reasonable attorneys' fees, expenses, and costs of suit.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: February 28, 2025

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Philip L. Fraietta*
Philip L. Fraietta

Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646)-837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., 9th Floor
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: sbogdanovich@bursor.com

Attorneys for Plaintiff